MANUAL DE CARGOS

Dependencia:	División Centro Servicios de Soporte	**Área:**	División Centro Servicios de Soporte
Código del Cargo:	3019.01	**Código del Puesto:**	3019
Categoría:	23	**Nombre del Puesto:**	Jefe de Área
Nombre del Cargo:	Oficial de Seguridad Funcional de los Sistemas Informáticos	**Reporta a:**	Jefe División Centro Servicios de Soporte
Objetivo del Cargo:	Ejecutar labores profesionales en la planificación, organización, coordinación supervisión, monitoreo e implementación de los controles de las actividades relacionadas con la seguridad funcional de acceso a los datos y sistemas informáticos del Banco, así como de mantener la seguridad y la confidencialidad sobre la emisión y mantenimiento de las identificaciones de usuarios y contraseñas. Asimismo, revisar y atender requerimientos varios que sean asignados por la jefatura correspondiente y brindar apoyo en lo que solicite, en concordancia con la normativa y valores institucionales.		

MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES
			1. Dirigir, coordinar, controlar y evaluar el desarrollo e implementación de las actividades establecidas para el proceso con el objetivo de que se cumplan los planes de trabajo y proponer las acciones que se consideren adecuadas para lograr la eficiencia de los procesos.
			2. Establecer la normativa, estándares, procesos y procedimientos de seguridad funcional relacionada con el riesgo en el uso de acceso a los sistemas informáticos del Banco, estableciendo como punto central la estandarización de los perfiles del sistema T24 (Core Bancario).
			3. Definir, establecer, mantener, administrar, diseñar y gestionar la creación o ajustes de perfiles de usuario de los sistemas, acatando las mejores prácticas y principio de seguridad informática, sobre menor privilegio posible, de conformidad con la normativa interna y externa y la evaluada por los entes reguladores.
			4. Coordinar y mantener la interacción con todas las dependencias del Conglomerado que son usuarias de los sistemas informáticos del Banco, así como con las dependencias correspondientes, para garantizar que las acciones definidas en los perfiles sean congruentes con las funciones del rol que desempeñan.
			5. Mantener presencia activa en los Proyectos del Banco relacionados con la seguridad funcional de los sistemas informáticos, con el fin de asegurar la atención de normativa regulatoria e interna y analizar en su impacto los riesgos por el uso y los ajustes o creación de nuevos perfiles y actualización de los controles respectivos.
			6. Implementar un adecuado sistema de control de seguridad funcional de accesos a los sistemas basado en roles, que contenga las medidas necesarias para auditar, mantener y monitorear un registro de acceso a las transacciones sensitivas, con el propósito de proteger la información, generar reportes estadísticos y alertas, así como elaborar diferentes tipos de informes para análisis y mejora continua.
			7. Asesorar a los superiores, para que en coordinación con las Direcciones de Riesgo Corporativo, de las Bancas y de Gestión se establezca un proceso de realimentación para la mejora continua, en materia de seguridad funcional y el riesgo por el uso de privilegios de acceso a sistemas.
			8. Analizar y atender todas las solicitudes de requerimientos de ajustes y/o nuevos perfiles, de las diferentes dependencias del Conglomerado que requieren accesos a sistemas informáticos del Banco.
			9. Mantener interacción con las áreas de Tecnología de Información para la aplicación de la normativa que se establezca, que proporcione la seguridad y la confidencialidad sobre la emisión y mantenimiento de las identificaciones de usuarios y contraseñas en procesos normales y de excepción.
			10. Monitorear la utilización de los perfiles definidos para cada rol y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada de acceso a los sistemas informáticos.
			11. Planificar, dirigir y coordinar la revisión y evaluación periódica del cumplimiento de las políticas institucionales de seguridad de información, aplicable a la seguridad funcional, por el riesgo en el uso de los perfiles definidos para acceder a los sistemas, así como sugerir los cambios necesarios.
			12. Preparar y ejecutar un plan de concientización en seguridad funcional, relacionada con el riesgo por el uso de acceso a los sistemas informáticos y uso de privilegios para las áreas estratégicas que se definan para el Banco.
			13. Planificar y ejecutar la revisión periódica de los perfiles y su seguridad en coordinación con las dependencias usuarias del Conglomerado, con el fin de proponer ajustes que faciliten el uso adecuado de sus privilegios y derechos de acceso.
			14. Velar por la prueba de los esquemas de seguridad de acceso a los sistemas para cada perfil, con el fin de evaluar la fortaleza de la seguridad por los privilegios y derechos de acceso que se defina para cada uno, detectar las posibles amenazas y establecer planes de acción preventivos.
			15. Velar por la seguridad funcional de los sistemas que se administren en la dependencia.
			16. Coordinar con Seguridad Operativa Informática, la Oficialía de Cumplimiento, Dirección de Riesgo y Auditoría, los mecanismos que aseguren de manera apropiada que la seguridad en el acceso a los sistemas está diseñada y actualizada correctamente de acuerdo a la normativa vigente en el Conglomerado.
			17. Aplicar una metodología de análisis de riesgo para evaluar la seguridad funcional, por el riesgo en el uso de privilegios de acceso a los sistemas informáticos.
			18. Detectar y reportar los incidentes de seguridad de acceso, en coordinación con el Área de Seguridad Operativa Informática, para el análisis en la atención y solución de los problemas que se presenten.
			19. Establecer estrategias relacionadas con el análisis de situaciones de riesgo que afecten la integridad de la información por accesos indebidos o no controlados.
			20. Elaborar y dirigir los proyectos de seguridad funcional de accesos a los sistemas, relacionados con reingeniería de perfiles por cambios en estructura organizativa, funciones de áreas y/o nuevas funcionalidades.
			21. Atender las consultas de Directores de área, Jefaturas, y Sociedades del Conglomerado, sobre aspectos relacionados con los accesos a sistemas requeridos por las áreas a su cargo.
			22. Implementar estrategias en materia de seguridad funcional, por riesgo en el uso de accesos a los sistemas para impartir capacitaciones a nivel institucional, relacionado con la congruencia entre roles, procesos y accesos enfocados en la seguridad en el uso para la mejora continua sobre la facilidad, tiempos de respuesta y satisfacción del cliente.
			23. Preparar y presentar los informes según la periodicidad definida sobre avances y comportamiento del desarrollo general de los procesos, emitir criterio profesional y recomendar las acciones correspondientes, exponer ante las instancias correspondientes.
			24. Colaborar y gestionar la ejecución de actividades establecidas en el Plan de Gestión de Seguridad de la Información, relacionada con aspectos de seguridad funcional.
			25. Ser miembro del Equipo Técnico de Seguridad del Conglomerado Financiero del Banco Popular y participar activamente de las sesiones periódicas.
			26. Planear, controlar, gestionar la elaboración de contratos con proveedores de dispositivos de firma digital y soporte técnico, así como los pagos correspondientes.

			27. Dar respuesta a informes, oficios, consultas, solicitudes y otros asuntos que requieran los entes supervisores internos y externos de manera que se realicen los procesos de evaluación y seguimiento requeridos.
			28. Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.
			29. Supervisar periódicamente el cumplimiento de los tiempos de respuesta establecidos para las funciones de su personal a cargo.
			30. Colaborar en la ejecución de actividades o proyectos establecidos de alcance Institucional para el Área, División o Dirección.
			31. Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
			32. Ejecutar otras funciones propias del Puesto, Área, División o Dirección.
			FUNCIONES RELACIONADAS CON RIESGO
			33. Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			34. Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			35. Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			36. Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			37. Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			38. Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			39. Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			40. En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
CODIGO	**REQUISITOS EXIGIBLES**		
	Formación Académica:	Licenciatura en Administración de Empresas o con énfasis en Banca, Finanzas, Gerencia; Informática; Ingeniería de Sistemas; Sistemas de Información. Preferiblemente con una Maestría en Sistemas de Información.	
	Legales:	Incorporado al Colegio Profesional respectivo y estar al día con sus obligaciones.	
	Experiencia:	Tres años de experiencia en labores relacionadas con la gestión de Seguridad Funcional en los sistemas de Información, Procesos de Seguridad de la Información, Seguridad de Sistemas o Procesos Riesgo Informático.	
CODIGO	*** REQUISITOS TÉCNICOS EXIGIBLES**		
	1. Conocimientos de inglés técnico.		
	2. Conocimientos de los esquemas de Seguridad Funcional de los Sistemas Informáticos.		
	3. Conocimiento en la Normativa relacionada con Seguridad de la Información.		
	4. Conocimiento en la Normativa de Riesgo Informático.		
	5. Conocimiento de herramientas de Office. Excell nivel avanzado.		
	6. Conocimientos de Administración de Riesgo Operativo y Riesgos en Tecnologías de la Información.		
	7. Conocimiento del Marco Metodológico Cobit 5.0 o Superior.		
	8. Conocimiento en el manejo de Herramientas Project.		
	9. Conocimiento de las Normas ISO 27001 y 27002.		
*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.**			
CODIGO	**REQUISITOS TÉCNICOS DESEABLES**		
	1. Conocimiento en Leyes y reglamentos que regulan la seguridad bancaria y del país: Ley Control Interno, Ley 8204, Reglamento Contratación Administrativa, Código de Trabajo.		
	2. Conocimiento en la elaboración de planes de trabajo y anteproyectos de presupuesto.		
	3. Conocimiento en capacitaciones técnicas de administración de la seguridad funcional en T24, así como de los demás sistemas informáticos.		
	4. Conocimientos de la funcionalidad del sistema T24.		
	5. Conocimiento en la implementación, gestión y/o auditoría del riesgo en Seguridad de la Información.		
	6. Conocimiento en la Normativa externa relacionada con la Superintendencia General de Entidades Financieras (SUGEF).		
	7. Conocimiento en la Normativa Interna del Conglomerado Financiero.		
	8. Conocimiento en el Manual de Normas de Atención y Servicio al Cliente.		
	9. Conocimiento en la Normativa externa relacionada con el Cumplimiento de la Ley 8204.		
CODIGO	**SISTEMAS UTILIZADOS**		
	Word, Excel, Power Point, Outlook		
	Sistema T24 y módulo de seguridad		
	Siscard módulo de seguridad		
	Sistema Sugef (módulo seguridad para CIC, NOTIFICACIONES, SICVECA)		
	SINPE. (nodo seguridad de FIRMA DIGITAL)		
	SIPRE. Sistema Integrado de Presupuesto		

	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL: JEFATURAS SOPORTE			
CÓDIGO	**Cardinales:**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CÓDIGO	**Gerenciales:**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CÓDIGO	**Del Negocio:**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CÓDIGO	**Del Soporte:**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CÓDIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Este perfil se crea según oficio DIRCH-111-2016 aprobado por la GGC.** **Se agregan las funciones Relacionadas con Riesgo, según autorización brindada por la Gerencia General Corporativa mediante HT-493-GGC-2019, de fecha 14 de octubre de 2019.** **La Gerencia General Corporativa aprueba ajustes a este perfil mediante oficio GGC-1943-2020, con fecha 29 de diciembre de 2020. Referencia DIRCH-1722-2020.**				